IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ASHLEY SALAS, individually and on behalf of all others similarly situated, Plaintiff, v. ACUITY-CHS, LLC d/b/a COMPREHENSIVE HEALTH SERVICES, LLC Defendant.	Civil Action No. 22-317-RGA

MEMORANDUM OPINION

Peter Bradford deLeeuw, DELEEUW LAW LLC, Wilmington, DE; Nicholas A. Migliaccio, Jason Rathod, Tyler J. Bean (argued), MIGLIACCIO & RATHOD, LLP, Washington, D.C.

Attorneys for Plaintiff.

Aimee M. Czachorowski, Cheneise Wright, Francis G.X. Pileggi, LEWIS BRISBOIS BISGAARD & SMITH LLP, Wilmington, DE; Danielle E. Stierna (argued), Jon P. Kardassakis, LEWIS BRISBOIS BISGAARD & SMITH LLP, Los Angeles, CA.

Attorneys for Defendant.

March 30, 2023

ANDREWS, UNITED STATES DISTRICT JUDGE:

Before me is Defendant's motion to dismiss. (D.I. 12). The motion has been fully briefed, and I have considered the parties' briefing. (D.I. 13, 15, 16). I held helpful oral argument on December 19, 2022. (D.I. 31). For the following reasons, Defendant's motion is GRANTED in part and DENIED in part.

I. BACKGROUND

This case arises from a data breach. Defendant Acuity-CHS, LLC d/b/a Comprehensive Health Services, LLC offers medical management solutions, including occupational health management services, for the U.S. Department of Homeland Security. (D.I. 10 at 7). Plaintiff Ashley Salas used CHS's services when she applied for a job at the U.S. Customs and Border Patrol Agency between late 2018 and early 2019, and again when she applied for a job at the Transportation Security Administration in 2021. (*Id.* at 5). As a part of the employment screening process, CHS administered medical examinations through a clinic in California. (*Id.*). To receive those examinations, Ms. Salas gave CHS certain private information. (*Id.*). CHS stored this information in its database. (*Id.*).

On September 30, 2020, CHS was the victim of a cyberattack. (*Id.* at 2). After discovering "fraudulent wire transfers," CHS "detected unusual activity within its digital environment and promptly launched an investigation" to determine the cause, as well as to identify information that may have been accessed or acquired without permission. (*Id.* at 9). On November 3, 2021, CHS learned that some information—specifically, the names, dates of birth, and Social Security numbers of at least 106,752 patients who had received CHS's services, including Ms. Salas—may have been compromised in connection with the data breach. (*Id.* at 9-10). On February 11, 2022, CHS published a Notification of Data Security Incident, which informed potentially affected

individuals of the breach and explained, "There is no evidence of the misuse of any information potentially involved in this incident." (*Id.*).

Ms. Salas now brings this putative class action in an amended complaint against CHS on behalf of herself and all others similarly situated. (D.I. 10). Her proposed nationwide class comprises "[a]ll persons whose Private Information was compromised as a result of the Data Breach discovered on or about September of 2020 and who were sent notice of the Data Breach." (*Id.* at 48). She asserts claims for negligence (Count I), breach of express contract (Count II), breach of implied contract (Count III), unjust enrichment (Count IV), violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10 *et seq.* (2008) (Count V), violation of California's Unfair Competition Law, Cal. Bus. Prof. Code § 17200 *et seq.* (Count VI), and violation of the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.* (Count VII). (*Id.* at 53-74). She also seeks a declaratory judgment "concluding that CHS owed, and continues to owe, a legal duty to employ reasonable data security to secure the Sensitive Information," and "prospective injunctive relief requiring [CHS] to employ adequate security practices consistent with law and industry standards to protect consumer and patient private information" (Count VIII). (*Id.* at 75-78).

Ms. Salas alleges that CHS's failure to secure her private information put her "at a serious, immediate, and ongoing risk of … fraud and identity theft." (*Id.* at 3). One such attempt, she claims, has already taken place. (*Id.* at 6). On February 28, 2022, Ms. Salas's identity theft protection software notified her that her email address had been used in an identity theft attempt. (*Id.*). Ms. Salas also alleges that the breach "resulted in costs and expenses … associated with the time spent addressing and attempting to ameliorate" the release of the information, as well as "the emotional grief associated with the substantial and imminent risk of falling victim to identity theft

and having to constantly monitor personal banking and credit accounts." (*Id.*). She alleges future injuries as well, which include mitigation costs, stress, and the loss of property value of her personal information. (*Id.*).

II. LEGAL STANDARD

A. Rule 12(b)(1)

Federal Rule of Civil Procedure 12(b)(1) permits the dismissal of a claim or an action for lack of subject matter jurisdiction. A Rule 12(b)(1) motion may be treated as either a facial or factual challenge to the court's subject matter jurisdiction. *See Davis v. Wells Fargo,* 824 F.3d 333, 346 (3d Cir. 2016). A facial attack contests the sufficiency of the pleadings, whereas a factual attack contests the sufficiency of jurisdictional facts. *See Lincoln Ben. Life Co. v. AEI Life, LLC*, 800 F.3d 99, 105 (3d Cir. 2015). When considering a facial attack, the court accepts the plaintiff's well-pleaded factual allegations as true and draws all reasonable inferences from those allegations in the plaintiff's favor. *See In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 633 (3d Cir. 2017). When reviewing a factual attack, the court may weigh and consider evidence outside the pleadings, *see Gould Elecs. Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000), and the party asserting subject matter jurisdiction bears "the burden of proof that jurisdiction does in fact exist." *Id.*

B. Rule 12(b)(6)

When reviewing a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6), the Court must accept the complaint's factual allegations as true. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555–56 (2007). Rule 8(a) requires "a short and plain statement of the claim showing that the pleader is entitled to relief." *Id.* at 555. The factual allegations do not have to be detailed, but they must provide more than labels, conclusions, or a "formulaic recitation" of the claim

elements. *Id.* ("Factual allegations must be enough to raise a right to relief above the speculative level … on the assumption that all the allegations in the complaint are true (even if doubtful in fact)."). Moreover, there must be sufficient factual matter to state a facially plausible claim to relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The facial plausibility standard is satisfied when the complaint's factual content "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* ("Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." (cleaned up)).

III. DISCUSSION

CHS makes approximately nineteen distinct arguments in its twenty-page opening brief. (D.I. 13). Unsurprisingly, these arguments are not fully developed in the briefing. Prior to oral argument, in compliance with my order (D.I. 23), CHS identified the five arguments that it considers most important. (D.I. 26). The five arguments are as follows: (1) Ms. Salas fails to meet the injury-in-fact requirement for Article III standing; (2) Ms. Salas fails to meet the traceability requirement for Article III standing; (3) Ms. Salas's negligence claim is barred by the economic loss doctrine; (4) Ms. Salas fails to state a claim for breach of contract "because she has not identified the terms of the alleged contract, formation of a contract based on those terms, or damages resulting from a breach of those terms"; and (5) Ms. Salas fails to state a claim for unjust enrichment "because she has not conferred a benefit directly on CHS, the retention of which by CHS was unjust." (*Id.*). These were the arguments that the parties developed at oral argument. (D.I. 31). The other arguments I hereby dismiss as cursorily made and without prejudice to being raised at the summary judgment stage.

A. Article III Standing

CHS argues that Ms. Salas's claims fail for lack of standing. (D.I. 13 at 4-7). I disagree.

Article III Standing to sue is a threshold requirement in every federal case. *Warth v. Seldin*, 422 U.S. 490, 498 (1975). Standing is necessary for subject matter jurisdiction. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157-58 (2014). To establish standing, a plaintiff must demonstrate: "(1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief." *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). CHS challenges the first two standing requirements.

"Standing is meant to serve as 'an essential and unchanging part of the case-or-controversy requirement of Article III,'" and is therefore "analytically distinct from the merits of the underlying dispute." *Davis*, 824 F.3d at 348 (quoting *Lujan*, 504 U.S. at 560). The Third Circuit has "repeatedly cautioned against allowing a Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction to be turned into an attack on the merits." *Davis*, 824 F.3d at 348 (discussing standing). Only in "narrow categories of cases" may courts dismiss under Rule 12(b)(1) for merits-related defects. *Id.* at 349-50. Courts may do so 'where the alleged claim under the Constitution or federal statutes clearly appears to be immaterial … or where such a claim is wholly insubstantial and frivolous.'" *Id.* at 350 (quoting *Bell v. Hood*, 327 U.S. 678, 682-83 (1946)). "[W]hen a case raises a disputed factual issue that goes both to the merits and jurisdiction, district courts must 'demand less in the way of jurisdictional proof than would be appropriate at a trial stage.'" *Id.*

Thus, in reviewing facial challenges to standing, I am limited to "a screening for mere frivolity" and must take care not to conflate the standing inquiry with an assessment of the merits

of Plaintiff's claim. *Adam v. Barone*, 41 F.4th 230, 234 (3d Cir. 2022). Factual challenges to standing—which flip the burden of persuasion to the plaintiff and allow a defendant to attack the allegations in the complaint using contrary evidence, all without the procedural safeguards of Rule 12(b)(6)—pose a particular risk of prejudice to the plaintiff. *See Davis*, 824 F.3d at 348-49. Consequently, and in light of the "tightly circumscribed" category of cases in which courts may dismiss for lack of jurisdiction based on merits considerations, "dismissal via a Rule 12(b)(1) factual challenge to standing should be granted sparingly." *Id.* at 350.

1. Injury-in-fact

"To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (quoting *Lujan*, 504 U.S. at 560). At the motion to dismiss stage, "the injury-in-fact element is not Mount Everest." *Blunt v. Lower Merion Sch. Dist.*, 767 F.3d 247, 278 (3d Cir. 2014) (cleaned up). The contours of this standard "are very generous"; Plaintiffs must only allege "some specific, identifiable trifle of injury." *Id.* (internal quotation marks omitted).

CHS argues that the injuries that Ms. Salas alleges are neither concrete nor imminent. (D.I. 12 at 4-5). I address each requirement in turn.

a. Imminence

To satisfy the injury-in-fact requirement, the alleged injury must be "actual or imminent, not conjectural or hypothetical." *Spokeo*, 578 U.S. at 339 (internal quotation marks omitted). "That 'actual or imminent' is disjunctive is critical: it indicates that a plaintiff need not wait until he or she has *actually* sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent." *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152 (3d Cir.

2022). For imminence, allegations of future injury "suffice if the threatened injury is 'certainly impending' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List*, 573 U.S. at 158 (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)).

The Third Circuit recently addressed the injury-in-fact requirement in the data breach context in *Clemens*, 48 F.4th at 152-59. In *Clemens*, a known hacking group infiltrated the defendant's servers, stole sensitive information pertaining to the plaintiff and others, held the information for ransom, and ultimately published that information on the Dark Web. *Id.* at 150. The plaintiff alleged a variety of injuries, first and foremost being an increased risk of identity theft and fraud. *Id.* at 151. The Third Circuit explained that, in determining whether such an injury is imminent or hypothetical, courts should consider the following factors: (1) whether the data breach was intentional, (2) whether the data was misused, and (3) "whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft." *Id.* at 153-54. These factors are non-exhaustive, and no single factor is dispositive to the inquiry. *Id.* at 153. Notably, the Third Circuit explained that the second factor—misuse—is "not necessarily required." *Id.* at 154 (citing *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007), in which the Seventh Circuit held there was standing despite no allegations of misuse). Applying the factors, the Third Circuit held that the plaintiff's allegations of future injury were sufficiently imminent. *Id.* at 157. The court noted that the hackers "*intentionally* gained access to and *misused* the data" by publishing it online, and that the compromised data—a combination of financial and personally identifying information—were "the type of data that could be used to perpetrate identity theft or fraud." *Id.*

Ms. Salas alleges that her private information was "accessed and viewed … with the intent of selling it and/or using it fraudulently to profit from such use." (D.I. 10 at 11). Ms. Salas alleges

actual misuse of her private information. She claims that it is "for sale to criminals on the dark web" (*id.*), and that the risks associated with such misuse—such as attempted identity theft—have already begun to materialize. (*Id.* at 6). In particular, Ms. Salas alleges that, in February 2022, she "received an alert through her identity theft monitoring service that her email address had recently been used in a potential identity theft incident." (*Id.* at 46). Furthermore, the nature of the information here is sensitive. Indeed, the *Clemens* court recited "social security numbers, birth dates, and names"—the personal information at issue in this case—as examples of information that is "more likely to create a risk of identity theft or fraud" if compromised. 48 F.4th at 154. Thus, like the plaintiff in *Clemens*, Ms. Salas has alleged a future injury that is sufficiently imminent.

CHS disagrees. (D.I. 13 at 5). It argues that this case is distinguishable from *Clemens*, and that the facts here more closely resemble those in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), another data breach case in which the Third Circuit held that the plaintiff's allegation of future harm was insufficiently imminent for standing. *Id.* at 46. There, the plaintiffs alleged a risk of future identity theft or fraud stemming from a data breach in which an unknown hacker potentially accessed sensitive personal and financial information (including names, Social Security numbers, and birth dates) from the defendant's computer network. *Id.* at 40. The plaintiffs did not allege any actual misuse. *Id.* at 43. The Third Circuit found that plaintiffs' alleged risk was too hypothetical for standing purposes; the risk depended on "entirely speculative, future actions of an unknown third party." *Id.* at 42 ("Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names.").

CHS argues that, like the plaintiffs in *Reilly*, Ms. Salas does not allege actual misuse of her information. (D.I. 12 at 5). This portion of CHS's argument, as I understand it, attacks the sufficiency of Ms. Salas's pleadings without disputing the facts alleged, and therefore constitutes a facial challenge. *See Davis*, 824 F.3d at 346. Accepting the allegations of the complaint as true and drawing all reasonable inferences in Ms. Salas's favor, as I must do when presented with a facial challenge to subject matter jurisdiction, *id.*, I come to the opposite conclusion. Unlike the *Reilly* plaintiffs, Ms. Salas has alleged actual misuse. (*E.g.*, D.I. 10 at 11 ("Plaintiff's and Class members' Private Information is for sale to criminals on the dark web")). Besides, as the Third Circuit recently stated, "misuse is not necessarily required" to establish injury-in-fact in a data breach case. *Clemens*, 48 F.4th at 154. Where misuse is absent, the presence of other factors may nevertheless confer standing. *Id.* Those other factors are present here, to varying degrees. Ms. Salas alleges that unauthorized parties intentionally accessed her data[1] (D.I. 10 at 11), and that those data include sensitive information, such as her Social Security number, birth date, and first and last name. (*Id.*). I therefore conclude that Ms. Salas has alleged an injury that is sufficiently imminent for standing.

[1] CHS argues that Ms. Salas has not satisfied this factor, as the intent of the breach was wire fraud (i.e., to steal money electronically from CHS), not identity theft. (D.I. 16 at 3; D.I. 31 at 15-16). CHS points to CHS's Notification of Data Security Incident, which Ms. Salas included in her Complaint. (D.I. 10 at 9-10). The Notification of Data Security Incident stated that information belonging to Ms. Salas and others may have been impacted in connection with an incident involving "unusual activity within its digital environment following discovery of fraudulent wire transfers." (*Id.*). Thus, says CHS, "the scheme here was to perpetuate wire transfer fraud against CHS." (D.I. 16 at 3).

I understand CHS's argument here to be a component of its facial challenge to standing. I therefore accept Ms. Salas's well-pleaded factual allegations as true and draw all reasonable inferences from those allegations in her favor. *See in re Horizon*, 846 F.3d at 633. Applying this standard, I find that it is reasonable to infer that a malicious third party who intentionally infiltrated CHS's system to use CHS's financial data to steal from CHS would also target the private data of Ms. Salas and others.

b. Concreteness

For concreteness, the central inquiry is "whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2200 (2021). Where a suit is premised on "the mere risk of future harm," a court must consider the type of relief sought. *Id.* at 2210-11. If the plaintiff seeks injunctive relief, the allegation of a risk of future harm can qualify as concrete, if the risk is "sufficiently imminent and substantial." *Id.* at 2210. But in a suit for damages, an allegation of a risk of future harm, standing alone, is insufficient; such plaintiffs must also allege that "the exposure to the risk of future harm itself causes *separate* concrete harm" in order to satisfy concreteness. *Id.* at 2211.

The Third Circuit has stated that, "in the data breach context, where the asserted theory of injury is a substantial risk of theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms." *Clemens*, 48 F.4th at 155-56. A plaintiff sufficiently supports such harms by alleging that, for example, "the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services." *Id.* Such was the case in *Clemens*, in which the plaintiff alleged "emotional distress and related therapy costs and the time and money involved in mitigating the fallout of the data breach." *Id.* at 158. The Third Circuit held that the plaintiff's alleged injury was sufficiently concrete. *Id.* (noting that "the harm involved is sufficiently analogous to harms long recognized at common law like the 'disclosure of private information.'" (citing *TransUnion*, 141 S. Ct. at 2204)). Here, Ms. Salas alleges the same additional harms. Among other things, she alleges "[a]nxiety and distress" due to her fear that her private information will be misused (D.I. 10 at 48), and "[c]urrent

and future costs in terms of time, effort and money" spent mitigating the impact of the data breach. (*Id.* at 47-48). I have already concluded that her injury is "sufficiently imminent and substantial." *Clemens*, 48 F.4th at 2210. Accordingly, I conclude that Ms. Salas has alleged an injury that is concrete enough for standing.

2. Traceability

CHS contends that Ms. Salas has failed to satisfy the traceability requirement for standing, as the potential misuse of Ms. Salas's email address is not fairly traceable to CHS's conduct. (D.I. 12 at 7). CHS's argument is that, because Ms. Salas's email address was not affected by the data breach, she cannot draw a causal connection between the alleged misuse of her email address and CHS's conduct. (*Id.*). For support, CHS offers the declaration of Jeffrey Rupert, senior legal counsel of CHS's parent company. (D.I. 13-1, Ex. A). CHS points to Mr. Rupert's statement that the information compromised in the data security incident did not involve Ms. Salas's email address. (*Id.* at 2). In response, Ms. Salas points to the "mosaic effect," by which cybercriminals piece together multiple data sources to reveal new private information about individual. (D.I. 10 at 6, 30-31; D.I. 15 at 8). She asserts that this is how identity thieves obtained her email address—by using the information compromised in the data breach. (D.I. 10 at 6). CHS counters that this argument is not plausible, as someone attempting identity theft who has accessed the victim's Social Security number would have no reason to use the victim's email address. (D.I. 16 at 1).

As CHS asks me to weigh and consider evidence outside the pleadings, its argument constitutes a factual attack, rather than a facial attack, on standing. *See Gould Elecs.*, 220 F.3d at 176. The disputed factual issue—the relationship between CHS's conduct and the alleged misuse of Ms. Salas's email address—"goes both to the merits and jurisdiction." *See Davis*, 824 F.3d at 350. I may grant such challenges where the plaintiff's claim "is wholly insubstantial and

frivolous." *Bell*, 327 U.S. at 682-83. Such seems to be the case here. Although the traceability requirement "'does not mean that plaintiffs must show to a scientific certainty that defendant's [actions], and defendant's [actions] alone, caused the precise harm suffered by plaintiffs,'" *Interfaith Cmty. Org. v. Honeywell Int'l, Inc.*, 399 F.3d 248, 257 (3d Cir. 2005) (cleaned up), plaintiffs must nevertheless show that their injuries "relate directly" to the defendant's conduct. *See id.* As I do not think Ms. Salas's "mosaic effect" theory amounts to more than mere speculation regarding CHS's involvement in the attempted identity theft incident regarding her email address, I do not think that the email incident is "fairly traceable" to CHS.

This conclusion, however, does not help CHS. As Ms. Salas points out (D.I. 31 at 25), CHS's traceability argument only addresses the narrow issue of misuse as it relates to Ms. Salas's email address. Ms. Salas makes other allegations of misuse, including misuse of the information directly impacted by the data breach—her name, date of birth, and Social Security number—which she alleges are "for sale on the Dark Web." (D.I. 10 at 11). And Ms. Salas need not allege actual misuse for standing purposes, provided that other factors recited in *Clemens*—such as the intent of the breach and the nature of the compromised information, 47 F.4th at 153-54—weigh in her favor. As discussed, I believe that they do.

Accordingly, I conclude that Ms. Salas has Article III standing, and I deny CHS's motion to dismiss her claims for lack of standing.

B. Negligence

Defendant argues that Plaintiff's negligence claim is barred by Delaware's economic loss doctrine. (D.I. 12 at 9-10).[2] That doctrine precludes a party from bringing a negligence claim if the

[2] Plaintiff brought this action under 28 U.S.C. § 1332(d)(2). (D.I. 10 at 7). "A federal court sitting in diversity applies the choice-of-law rules of the forum state … to determine the controlling law." *Maniscalco v. Brother Intern. (USA) Corp.*, 709 F.3d 202, 206 (3d Cir. 2013).

alleged losses are only economic in nature—i.e., "divorced from any injury to person or property." *Bray v. Gamestop Corp.*, 2018 WL 11226516, at *4 (D. Del. Mar. 16, 2018). Delaware courts have defined economic loss as "any monetary loss, costs of repair or replacement, loss of employment, loss of business or employment opportunities, loss of good will, and diminution in value." *McKenna v. Terminex Intern Co.*, 2006 WL 1229674, at *4 (Del. Super. Ct. Mar. 13, 2006).

The purpose of the economic loss doctrine is to preclude tort claims "where overlapping claims based in contract adequately address the injury alleged." *Brasby v. Morris*, 2007 WL 949485, at *6 (Del. Super. Ct. Mar. 29, 2007). The doctrine's underlying principle is "the notion that contract law provides a better and more specific remedy than tort law." *Id.* As such, Delaware courts have held that tort and contract claims might coexist where "a defendant breached a duty that is independent of the duties imposed by the contract." *McKenna*, 2006 WL 1229674 at *2. As Ms. Salas does not argue that she has claimed a breach of a duty independent of the contractual obligations central to her breach of contract claims, I do not address that issue here.

The economic loss doctrine bars Ms. Salas's negligence claims to the extent that her claims are for purely economic losses. CHS argues that her negligence claims are for purely economic losses and are therefore barred. (D.I. 13 at 9). Ms. Salas argues that she has alleged certain non-economic losses. (D.I. 31 at 51). First, she says that the alleged loss of value of her private information is a non-economic injury to property and thus lies beyond the scope of the economic loss doctrine. (*Id.* at 51-52). I disagree. This court has held that diminution of the value of personal

---

Both parties' briefs cite Delaware law. (*See, e.g.*, D.I. 13 at 9-10; D.I. 15 at 12-14). Thus, without deciding the choice of law issue, I will presume that Delaware law applies. *See Zazzali v. Hirschler Fleischer, P.C.*, 482 B.R. 495, 517 (D. Del. 2012) ("Due to the complexity of [the choice of law] analysis, when confronted with a choice of law issue at the motion to dismiss stage, courts within the Third Circuit have concluded that it is more appropriate to address the issue at a later stage in the proceedings.").

information is an economic loss, rather than property damage. *Bray*, 2018 WL 11226516 at *4 (dismissing negligence claim in data breach case as barred by Delaware's economic loss doctrine). Ms. Salas cites to *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447 (D. Md. 2020) for the proposition that "the growing trend across courts … is to recognize the lost property value of [personal] information." *Id.* at 460-61. The *Marriott* Court, however, said this in the context of its Article III standing analysis. *Id.* The Court ultimately declined to decide the economic loss doctrine issue, *id.* at 476, and in any event, its discussion of that doctrine was in the context of Illinois law. *See id.* at 467-76. Thus, I think that case is inapplicable here.

Ms. Salas also argues that her allegations based on emotional harm are non-economic. (D.I. 31 at 51). CHS counters that these allegations are insufficient because Ms. Salas does not support them with allegations of physical injury. (D.I. 13 at 10). "It is settled law in Delaware that, in a negligence action, for a claim of mental anguish to lie, an essential ingredient is present and demonstrable physical injury." *Collins v. African Methodist Episcopal Zion Church*, 2006 WL 1579718, at *6 (Del. Super. Ct. Mar. 31, 2006); *see also Brzoska v. Olson*, 668 A.2d 1355, 1362 (Del. 1995). Counter to Ms. Salas's assertions at oral argument (D.I. 31 at 52-53), neither "the emotional grief associated with the substantial and imminent risk or falling victim to identity theft and having to constantly monitor personal banking and credit accounts" (D.I. 10 at 3) nor "the stress, nuisance, and aggravation of dealing with all issues resulting from the Data Breach" (*id.*) constitute physical harm. I agree with Defendant that the cases that Ms. Salas relies upon in support for such damages being recoverable are inapposite. (D.I. 16 at 6). Both cases—*Dannunzio v. Lib. Mut. Ins. Co.*, 2021 WL 5177767 (E.D. Pa. Nov. 8, 2021) and *TransUnion*, 141 S. Ct. 2190 (2021)—involved Fair Credit Reporting Act (FCRA) claims, rather than negligence, and neither

case involved Delaware law.[3] Thus, Ms. Salas's arguments with respect to emotional harm fail as well.

I therefore grant CHS's motion to dismiss Count I.

C. Breach of Contract Claims

CHS argues that Ms. Salas has failed to state a claim for breach of contract. (D.I. 13 at 11-12). I agree with respect to Ms. Salas's breach of express contract claim, but not with respect to her breach of implied contract claim.

To survive a motion to dismiss for failure to state a breach of contract claim, the plaintiff must demonstrate: "(1) the existence of an express or implied contract; (2) a party breached the obligation imposed by the contract; and (3) any damages that the plaintiff incurred as a result of the breach." *Saunders v. E.I. duPont de Nemours & Co.*, 2014 WL 7051078, at *4 (D. Del. Dec. 12, 2014). An express contract is expressed in writing or orally, whereas an implied contract "is proven through conduct rather than words." *Chase Manhattan Bank v. Iridium Africa Corp.*, 239 F. Supp. 2d 402, 407 (D. Del. 2002).

Ms. Salas's second and third claims assert a breach of express contract, (D.I. 10 at 58-61), and, in the alternative, a breach of implied contract. (*Id.* at 61-66). As an initial matter, I disagree with CHS's argument that these claims are mutually exclusive. (D.I. 13 at 12). CHS cites *Chase Manhattan Bank*, in which the court held that "a party may not simultaneously allege an implied-

[3] Similar problems arise with respect to the other cases Ms. Salas cites in support of her negligence claims. Ms. Salas cites *Frunzi v. Paoli Servs., Inc.*, 2012 WL 2691164 (Del. Super. Ct. July 6, 2012) for the proposition that "once a plaintiff establishes that a defendant breached the duty of care, the defendant is liable for all consequential damages flowing from that breach." (D.I. 15 at 12). But the cited analysis in *Frunzi* pertained only to damages for breach of contract and did not involve emotional harms. *Id.* at *8. And Ms. Salas cites *Opris v. Sincera Reprod. Med.*, 2022 WL 1639417 (E.D. Pa. May 24, 2022) for the proposition that mitigation costs stemming from a data breach are compensable in negligence. (D.I. 15 at 13). But that case involved Pennsylvania law, *id.* at *3, and the economic loss doctrine was not at issue.

in-fact and express contract based on the same terms or embracing the same subject matter." 239 F. Supp. 2d at 408. That case, however, is inapposite. There, the dispute arose at the summary judgment stage, and the court based its decision on the impracticalities of presenting both theories at trial. *Id.* at 410-11. Here, at the motion to dismiss stage, Ms. Salas may allege both claims as alternative theories of recovery. *See* FED. R. CIV. P. 8(d)(2)-(3).

1. Breach of Express Contract

In her complaint, Ms. Salas alleges that the parties entered an express contract "under which Plaintiff and other class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide medical exam services and protect Plaintiff and Class members' Private Information." (D.I. 10 at 58-59). Ms. Salas derives this contract from multiple "express contracts" between Ms. Salas and CHS—specifically, she identifies "HIPAA privacy notices and explanation of benefits documents" (*id.* at 59), as well as a presentation made by CHS's parent company in May 2020. (*Id.* at 31).

CHS contends that Ms. Salas's breach of express contract claim fails because she "fails to aver any particular contract terms that she contends [were] breached." (D.I. 13 at 11-12). I agree. Under Delaware law, a plaintiff bringing a breach of contract action must plead the existence of "sufficiently specific terms that determine the obligation of each party." *Tani v. FPL/Next Era Energy*, 811 F. Supp. 2d 1004, 1023 (D. Del. 2011). Ms. Salas fails to do so. She provides no detail as to the terms of the "HIPAA privacy notices and explanation of benefits documents"—she merely avers that these documents exist. (D.I. 10 at 59). Ms. Salas does provide portions of the May 2020 presentation by CHS's parent company, (*id.* at 12-13), but it is not clear from the allegations why this presentation matters; Ms. Salas does not say who the audience of this

presentation was, and in any event, the presentation was delivered by CHS's parent company, and not by CHS.

These allegations are not sufficient to allege a breach of express contract.[4] I therefore grant CHS's motion to dismiss Count II.

2. Breach of Implied Contract

CHS argues that, as with Ms. Salas's breach of express contract claim, Ms. Salas fails to allege the existence a contract, as she has not identified any particular contract term that CHS might have breached. (D.I. 12 at 11).

"[T]he elements required to form an implied-in-fact contract are identical to those required for an express agreement, that is offer, acceptance, and consideration." *Chase Manhattan Bank*, 239 F. Supp. 2d at 408. There must be a 'meeting of the minds,' and "the parties' mutual assent to the contract terms must be objectively manifest or shown." *Id.*

Ms. Salas alleges, "Through their course of conduct, Defendant, Plaintiff, and Class members entered into implied contracts for the provision of health care services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class members' Private Information." (D.I. 10 at 61). Ms. Salas alleges that she paid money (*id.* at 67) and gave her private information (*id.* at 58-59) in exchange for CHS's services.[5]

---

[4] I am unconvinced by Ms. Salas's argument that, "[b]ecause the parties' contractual intent relates to multiple documents, the express agreement is a question of fact that will need to be further explored in discovery." (D.I. 15 at 15-16). At issue here is the sufficiency of the factual allegations, not the sufficiency of the evidence, and Ms. Salas has failed to adequately allege that these documents constitute an express contract.

[5] CHS points to Mr. Rupert's declaration, in which he says, "Job applicants do not make any payments to CHS … for preplacement exams." (D.I. 13-1, Ex. A at 2). In its briefing, CHS makes no argument that Ms. Salas has failed to adequately allege the consideration element of her breach

Neither party cites to Delaware case law addressing this issue. Other courts have reached a variety of conclusions. *Compare Castillo v. Seagate Tech., LLC*, 2016 WL 2980242, at *9 (N.D. Cal. Sept. 14, 2016) ("While [Defendant] made no explicit promises as to the ongoing protection of personal information, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security Numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently."), *and In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (holding that the plaintiffs had sufficiently pleaded "an implied contract in which Plaintiffs agreed to use their credit or debit cards to purchase goods at Target and Target agreed to safeguard Plaintiffs' personal and financial information"), *with Lovell v. P.F. Chang's China Bistro, Inc.*, 2015 WL 4940371, at *3 (W.D. Wash. Mar. 27, 2015) (dismissing breach of implied contract claim in data breach case). As the question appears unsettled, in the interest of caution, I conclude that Ms. Salas has sufficiently pled the existence of an implied contract. *See Bray*, 2018 WL 11226516, at *6 (allowing plaintiffs'

---

of contract claim. Ms. Salas, in her opposition brief, appears to maintain that she paid for CHS's services. (*See* D.I. 15 at 18).

At oral argument, however, Ms. Salas conceded that, in view of Mr. Rupert's declaration, "it looks like there may not have been an exchange of money between Ms. Salas and CHS." (D.I. 31 at 32). CHS then raised a consideration challenge, arguing that Ms. Salas's private information is inadequate consideration for the alleged contract. (*Id.* at 43).

This argument, however meritorious it might be, is of no moment here. I must "accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." *Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 231 (3d Cir. 2008). Although I may consider "undisputedly authentic documents attached to a motion to dismiss" in making my determination, *Delaware Nation v. Pennsylvania*, 446 F.3d 410, 413 n. 2 (3d Cir. 2006), I may only do so if the claims in the complaint are "based" on the extrinsic document—otherwise, Defendant's motion must be treated as a motion for summary judgment. *Schmidt v. Skolas*, 770 F.3d 241, 249 (3d Cir. 2014) (cleaned up). As Ms. Salas did not use Mr. Rupert's declaration in framing her complaint, and as I do not think that treating CHS's motion as a motion for summary judgment is warranted, I decline to consider Mr. Rupert's declaration. I will therefore assume, for the purposes of this opinion, that Ms. Salas paid CHS for its services.

breach of implied contract claim to proceed at the motion to dismiss stage, reasoning that it is "prudent to proceed with caution at this early stage, especially with the lack of consensus among the courts"); *In re Rutter's Inc. Data Security Breach Litigation*, 511 F. Supp. 3d 514, 537 (M.D. Pa. 2021) (same).

CHS next argues that Ms. Salas has not sufficiently alleged that CHS breached any obligations under, for example, the HIPAA privacy notices and explanation of benefits documents, as these documents "do not guarantee that CHS's network will remain free from data breaches from third-party cybercriminals." (D.I. 13 at 12). But Ms. Salas does not allege that CHS made any such guarantee. What Ms. Salas alleges is that CHS promised to "reasonably protect [Plaintiff's] Private Information" and that "[its] data security practices complied with relevant laws and regulations, and were consistent with industry standards." (D.I. 10 at 62). Ms. Salas alleges that CHS breached this promise by choosing to "ignore" industry standards, (*id.* at 37), and "fail[ing] to comply with safeguards mandated by HIPAA regulations." (*Id.* at 33). These allegations are sufficient.

Finally, CHS contends that Ms. Salas has failed to allege damages resulting from the alleged breach. (D.I. 13 at 11-12). Ms. Salas alleges several damages theories in her complaint. First, she alleges "benefit of the bargain" damages—she "received healthcare and other services that were of a diminished value to that described in the contracts" as the result of CHS's failure to fulfill its data security promises, and she would not have provided her private information to CHS had CHS disclosed its security deficiencies. (D.I. 10 at 65). Second, she alleges "actual damages and injuries" including the release, disclosure, and loss of control of her private information, as well as the imminent risk of future damages, disruption of medical care and treatment, and out-of-pocket expenses. (*Id.* at 66.)

CHS contends that Ms. Salas's alleged "benefit of the bargain" damages do not properly support her claim, as "she has not shown the medical services she received or the level of protection of her information was worth less than what she expected when she provided her information." (D.I. 12 at 11). Ms. Salas replies that CHS's argument is immaterial because she is entitled to recover nominal damages for the breach of contract. (D.I. 15 at 17). This seems true enough. Under Delaware law, a party bringing a breach of contract claim must allege "first, the existence of the contract …; second, the breach of an obligation imposed by that contract; and third, the resultant damage to the plaintiff." *VLIW Tech., LLC v. Hewlett-Packard Co.*, 840 A.2d 606, 612 (Del. 2003). With respect to the third element, however, "[a] party need not plead cognizable damages," as "[a]ll that is required is cognizable harm, and the breach of a contract right gives rise to cognizable harm." *In re P3 Health Group Holdings, LLC*, 2022 WL 16548567, at *30 (Del. Ch. Oct. 31, 2022); *Garfield on behalf of ODP Corporation v. Allen*, 277 A.3d 296, 328 (Del. Ch. 2022) ("[A] plaintiff need not plead monetary damages to sustain a breach of contract claim. The plaintiff need only plead causally related harm, which the plaintiff can accomplish by pleading a violation of the plaintiff's contractual rights."). As already discussed, Ms. Salas has sufficiently pleaded breach of contract; I am therefore unmoved by CHS's argument as to her damages.

For the reasons stated above, I conclude that Ms. Salas has adequately stated a claim for breach of implied contract. I therefore deny CHS's motion to dismiss as to this claim.

D. Unjust Enrichment

CHS contends that Ms. Salas fails to allege an unjust enrichment claim. (D.I. 12 at 12-13). I disagree.

Unjust enrichment is "the unjust retention of a benefit to the loss of another, or the retention of money or property of another against the fundamental principles of justice or equity and good

conscience." *Fleer Corp. v. Topps Chewing Gum, Inc.*, 539 A.2d 1060, 1062 (Del. 1988). In Delaware, the elements of equitable claim of unjust enrichment are: "(1) an enrichment, (2) an impoverishment, (3) a relation between the enrichment and impoverishment, (4) the absence of justification, and (5) the absence of a remedy provided by law." *Nemec v. Shrader*, 991 A.2d 1120, 1130 (Del. 2010).

Ms. Salas alleges that CHS has wrongfully retained money that Ms. Salas paid in exchange for services that CHS—by failing to adequately safeguard Ms. Salas's private information—did not provide.[6] (D.I. 10 at 67-69). This is sufficient.

CHS's first argument to the contrary is that, because Ms. Salas's unjust enrichment claim is "based on the same conduct as the breach of conduct claims," Ms. Salas has not adequately alleged the absence of a legal remedy as required under the fifth element. (D.I. 12 at 12-13). At oral argument, Ms. Salas said that she pleads her unjust enrichment claim in the alternative to her breach of contract claims. (D.I. 31 at 59). She may do so. Under Delaware law, "it is permissible for a party to seek quasi-contractual relief in the alternative to its contract claims." *Hiller & Arban, LLC v. Reserves Mgmt., LLC*, 2016 WL 3678544, at *3 (Del. Super. Ct. July 1, 2016). Delaware state courts generally allow such alternative pleading "when there is doubt surrounding the enforceability or the existence of the contract." *Albert v. Alex. Brown Mgmt. Servs., Inc.*, 2005 WL 2130607, at *8 (Del. Ch. Aug. 26, 2005).[7] I think that is the case here. Thus, I am not persuaded by CHS's first argument.

---

[6] Ms. Salas does not allege in her complaint that her private information was a benefit conferred upon (and wrongfully retained by) CHS. This theory arose primarily at oral argument. (*See* D.I. 31 at 59-60).

[7] Furthermore, I am not sure that I am bound by state court practice. "[A] federal court hearing a diversity of citizenship action [that is, a claim based on state law] should not be bound by a state law requiring that an election be made at the pleading stage, because a local practice of this type

CHS's second argument is that Ms. Salas has not adequately alleged a relation between the enrichment and impoverishment, as is required under the third element. (D.I. 13 at 13). To the extent that CHS's argument is that Ms. Salas has not shown that her personal information constituted a "benefit" conferred to CHS (*see* D.I. 16 at 9), I am unconvinced. As discussed, I accept as true Ms. Salas's allegation that she paid CHS money for its services, and money certainly benefits CHS. CHS contends that even under this assumption, Ms. Salas's claim fails because she "has not shown the cost of the exam was higher because it included payment for data protection or that CHS's retention of payment for physical exam services provided is unjust." (D.I. 13 at 13). The case it relies upon for this point—*In re Am. Med. Collection Agency Customer Data Sec. Breach Litig.*, 2022 WL 5937742 (D.N.J. Dec. 16, 2021)—is inapposite. There, the court dismissed the plaintiffs' unjust enrichment claim because the plaintiffs failed to allege that the defendant was benefitted by collecting plaintiffs' personal data. *Id.* at *18. Here, CHS is alleged to have received Ms. Salas's money in addition to her personal information. (D.I. 10 at 67; *see also* D.I. 15 at 18). More to the point, as explained with regard to Ms. Salas's breach of implied contract claim, I believe that Ms. Salas has sufficiently alleged that the services she paid for included data security practices consistent with industry standards and compliant with relevant laws and regulations. This is sufficient to establish the requisite "relation" under the third element.

I will therefore allow Ms. Salas to proceed on her claim of unjust enrichment as an alternative theory of recovery to her breach of contract claim. Thus, I deny CHS's motion to dismiss Ms. Salas's unjust enrichment claim.

---

might cripple the flexible pleading provisions sanctioned by Rule 8(d)(2) and defeat the overriding federal policy of having disputes determined on their merits." 5 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE & PROCEDURE § 1283 (4th ed. 2022).

IV. CONCLUSION

An appropriate order will issue.